ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/97105 November 2016* ISSN (Online) : 0974-5645

VANET and its Security Aspects: A Review

Kirti A. Yadav and P. Vijayakumar

School of Electronics Engineering ,VIT University, Chennai Campus, Chennai – 600127, Tamil Nadu, India; yadavkirti.ankush2015@vit.ac.in, vijaya.kumar@vit.ac.in

Abstract

Objectives: This paper reviews research on various routing protocols used in Vehicular Adhoc Network (VANET), with the aim to 1. Examine the newly emerged routing strategies, 2. To identify the security aspect of these routing strategies, 3. To explore security importance to users and 4. To investigate the research direction for security in VANET. **Methods/Statistical Analysis:** This paper focuses on two major aspects which includes literature survey and review along with a conceptual analysis of VANET security aspects. For this 20 security in VANET related papers have compared and analyzed along with some basic paper on VANET and routing to provide security in vehicular adhoc network. **Findings:** The survey of this paper indicates that the security aspect for VANET secured communication requires successful accomplishment of all aspects. However, the recent survey concludes that there is still further scope for research in security aspects like integrity, non-repudiation, availability. **Application/Improvements:** This study (review) tries to suggest that understanding the approach of routing and will help to implement a better intelligent transport system with security.

Keywords: Routing Protocol, Security Study, Vehicular Adhoc Network

1. Introduction

Nowadays private transport is a daily necessity of human being. Due to an intensify use of private transport, road accidents have become a major problem approached by the modern society. Vehicular communication is one of the ways to decrease the hazardous accidents coming forth. Vehicular communication can be brought in existence by having a communication of one vehicle with other vehicle, which is commonly referred to as Vehicle to Vehicle communication (V2V) or also by communication with a specific fixed unit called as Road Side Unit (RSU). Not only this, accident can also be prevented if communication is established between Vehicle and nearby Infrastructure (V2I). All this communication can be generally referred to as inter vehicular communication. Thiscommunication allows vehicles to share various kinds of informationincluding safety information for the purpose of accident prevention; post-accident investigation or traffic jams and many more[1].Europe and North America are ahead in conducting research to finalize the standards for vehicular communication. It identifies technical specifications (for example, regarding radio frequencies and messaging formats) to enable communication among vehicles of different manufacturers and between vehicles and the road infrastructure[1]. One of the means of communication is through Dedicated Short Range Communication (DSRC) and also through WAVE i.e. Wireless Access in Vehicular Environments. DSRC is the medium through which all this communication takes effectively executed. The IEEE standard 802.11a is modified as IEEE 802.11p[2] for low overhead tasks. However, the decentralized nature of IEEE 802.11p imposes imitations on the reliability of the standard[3].The whole communication model is then combined and commonly referred as WAVE. Simple example of this type of communication is, suppose there are two vehicles, A1 and B1, travelling together. At a point, vehicle A1 speeds up and moves ahead of vehicle B1, but suddenly meets up with an accident. Now vehicle A1 does not want vehicle B1 to face the same problem. So then vehicle A1 can simply broadcast a message, which can act as an alert message for vehicle B1, thus preventing from accident.Not only vehicular communication prevents up accidents, but it can also be used for much other application like providing traffic related information, late

** Author for correspondence*

accident information, multimedia exchange, security, etc. It makes driving safer, smarter, and greener and more comfortable[4].Though VANET is part of MANET (mobile adhoc network), Due to the unique characteristics of VANETs, such as high mobility with an organized but constrained pattern, and diverse radio propagation conditions, the conventional researches dedicated for general MANETs cannot be directly applied to VANETs[5]. A variety of car manufacturers are providing vehicles with inbuilt on- board computing and wireless communication devices, along with in specific car sensors, and navigation systems like Global Positioning System (GPS) and Galileo in preparation for the enhancement of large-scale vehicular networks. By using different types of sensors (e.g., sensors for road and weather conditions, state of the vehicle, radar and others), cameras, computing and communication capabilities, vehicles can collective grasp and communicate information with the purpose of guiding the driver to make a decision[6]. Europe, Japan and also USA are undertaking many projects for the growth of vehicular communication and its security aspects[7,8]. Vehicle Safety Communications Consortium (VSCC) (USA), European automotive industry project co-funded by the European Communication Commission (ECC) to foster road safety through the development and demonstration of preventive safety-related applications/technologies called Prevent project and many more[9]. Recent research issues of VANET include authentication schemes, trust management mechanisms, attacks prevention, VANET clouds, security and privacy enhancement, position based VANET mechanisms, traffic management, VANETsecurity framework, routing protocolsand geocast based routing, cryptographic solutions, clustering algorithms,CR-VANET[10].

Due to the advancement in information technology and communication, the idea of networked vehicle has gained successive attention all over the world. Recent survey[11], tell that people will increase their need of mobility around 35% per decade for the next three decades. In these surroundings, Vehicular Adhoc Network will be gaining a vast increase in its research. Not only this, the different applications of VANETs like, acquiring data, sharing of resources, processing and transmission of data through VANET, will gain more complexity as the number of vehicles get increased in the connected network. These applications are moreover illustration of Intelligent Transport System (ITS), whose main goal is to provide improved safety, city awareness along with pleasure in transportation system. This can be achieved through the use of various advancement in information and communication.All inclusively we can say that Vehicular AdhocNetwork holds a significant importance in the increasingly fasten and ambulant world. Effectively it enhances the quality of travel, reduce traffic harms, diminish the influence of congestion and will provide pleasant and smooth driving experience.

The further paper can be broadly detailed as section 2 will describe VANET architecture, section 3 will give the brief idea about distinctive features of VANET , section 4will describe the VANET communication model, section 5 will describe various routing strategies, section 6 will give the idea of different protocols currently used for VANET security, section 7 will describe security aspects and challenges for VANET, section 8 will give the idea of various simulation platforms, section 9 will give future research direction for secured VANET communication.

2. Vehicular Adhoc Network Architecture

VANET aims at providing smart traffic management and enhances the quality of transport by making travelling safer, more synchronized and intelligent. VANETs differ from MANETs in many ways including high node mobilitycan handle large scale of networks, a geographically constrained topology that is highly dynamic, with strict real time deadline, unreliable channel conditions, unavoidably slow deployment, and sporadic connectivity between nodes, driver behavior and frequent network fragmentation[12]. Main target of vehicular communication is to establish communication between vehicles. For proper co-ordination between the vehicles, communication plays a very important role. This communication is divided into two main segments which are referred as Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I/ I2V). To establish this communication an intermediate source is placed which can effectively communicate either with nearby vehicle or with the nearby infrastructure. This mediator is referred to as Road Side Unit (RSU). It plays a major role in the entire communication model. In V2V communication a particular vehicle can receive as well as transmit information to other vehicles. Not only this they can also exchange any kind of data or any valuable traffic information. This sharing or transmitting of information between vehicles is to make aware of the latest traffic updates as well as to avoid accidents. In V2I / I2V communication, it can send or receive information following safety measures. This protects the passengers from unpredictable incidents. Here the RSU is the one who plays an important role to communicate with other networks such as internet as shown in Figure 1. V2I links are less vulnerable to attacks and require more bandwidth than V2V links[13]. The structure of VANET can be studied through Figure 1, which explains the major components of VANET.

In VANET architecture, the major role is of three main parts which includes vehicle (V), road side unit (RSU) and the infrastructure (I). RSU plays the role of a router as well as it also accomplishes the role to provide services to the nearby sections. On Board Unit (OBU) is mounted on the vehicle which can also be referred as GPS i.e. global positioning system in order to track the vehicle. Vehicle also consists of Electronics License Plate (ELP) along with some necessary sensors. OBU uses the services provided by the RSU. The entire communication between RSU and vehicle or between vehicle and nearby infrastructure or also between two vehicles is accomplished with help of vehicular communication IEEE 802.11p standards.

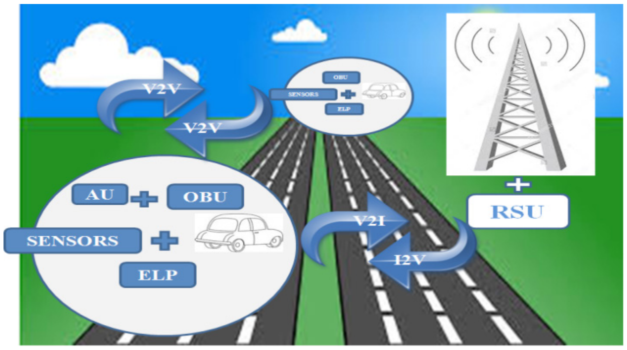

Figure 1. VANET Architecture overview.

2.1 Roadside Unit (RSU)

The unit kept aside the road for communication at regular intervals is called as Road Side Unit. These are normally placed at traffic nodes or also at parking areas. The RSU must be equipped with some of the standards of vehicular communication in order to have communication with supportive nearby infrastructure and vehicles. As RSU acts as a mediator, it plays many important roles in accomplishing the faithful communication. Following are its major roles.

- Establishing a small adhoc network and enhancing the range of communication by spreading the information to other RSU's and from them to other OBU's.
- Not only this it also provides accident warnings, traffic updates. It justacts like an informative source.
- Also provides internet facilities to nearby OBU's.
- The number of RSU's is dependent on the communication protocol that is to be used[7].

2.2 On-Board Unit (OBU)

When the vehicle wants to communicate with other vehicle or any nearby section, it needs some source through which it can communicate. This source is an OBU which is equipped with the vehicle. These OBUs are used to set up anadhoc network with various networks[14]. The OBUs and RSUs, equipped with onboard sensory, processing, and wireless communication modules, form a self-organized network with vehicles as nodes, commonly referred to as VANET[15]. This device should also support any vehicular communication standard similar to that with RSU. Like RSU, OBU also has some efficient functions. Wireless radio access, Adhoc geographical routing, Network congestion control, Reliable message transfer, Data security, IP mobility are the functions provided by OBU[16].Accordingto the ETSI 102 638 technical report, by 2017, 20%of all running vehicles will have communication capabilities,and they estimate that, by 2027, almost 100% of all vehicleswill be equipped with OnBoard Units (OBUs)[17].

2.3 Sensors

Sensors are used on the OBUs for sensing particular information based on the application design of the VANET. OBU is combined with some set of sensors in order to transfer the various updates to the RSU's. Not only this, it may also share current location of the vehicle through GPS. In general, sensors may include collision detection, moisture sensing, gas detection, and many more depending on various applications of VANET. Sensors may also be included of radar, cameras, GPS[18].

2.4 Application Unit (AU)

It a type of device that is built in order to utilize the different facilities provided by the RSU. It is generally mounted along with OBU. OBU fetches the facilities from RSU and provides to AU. The distinction between AU and OBU is logical[16], Different AUs can be interfaced with a single OBU simultaneously and with the help of this it can share the OBUs processing and wireless resources available. An AU communicates solely via the OBU, which is capable of handling all mobility and networking functions on the AUs' behalf.

2.5 Electronic License Plate(ELP)

It is the unique identity of the vehicle in order to locate or track the vehicle through global positioning system, during accidents or even missing of a particular vehicle.

3. Characteristic of VANET

VANET is having some unique characteristics as compared to that of a MANET[16,19]. These features emphases its advantages over MANET. Some of these features are included as follows.

3.1 Predictable Mobility

VANET differ other types of networks wherein in VANET, the nodes move in defined fashion as they are bounded to road topology constrains and vehicles have to obey road signs and the traffic signals. This adds on the unique characteristics of VANET in terms of predictable mobility.

3.2 Safe Driving, Traveler Comfort and Enhanced Traffic Competency

VANET establishes direct communications among mobile vehicles. Therefore, it is capable of providing alert or warning messages about accidents to drivers who are commencing their journey in the same direction, or may also provide a sudden message regarding hard breaking in case of landslides and any other calamity, informing the driver to be aware and construct a broader picture of the road ahead. Along with these additional kinds of applications could be applied for safety majors by the use of this type of network which regains passenger comfort and traffic efficiency by disseminating information about weather, traffic flow and along with this also some information related to point of interest of user (gas station, shopping malls and fast food).

3.3 No Power Constraints

Vehicles are capable of providing continuous power to the OBU through its battery. Therefore, no extra power is required to be maintained.

3.4 Variable Density Constraints

Density here defines the amount of vehicles at time in the network. In vehicular communication the amount of vehicles may differ depending upon the traffic scenario which may be either high or low at times.

3.5 Sudden Change in Network Topology

Every time it is not necessary that the vehicles may move at a constant speed. In a network here may be vehicles moving at high speed as well as vehicles moving at low speed. Even though there is a variation in the speed, VANET is capable of communicating through the network. Then communication link between the vehicles moving in opposite direction is very short as compared to that of vehicles moving in the same direction. The sudden changes in link connectivity cause the corresponding network diameter to be small; also many times some of the paths are disconnected before they can be used for communication.

3.6 Large Scale Networks

VANET is capable of establishing its network for crowed city areas as well as areas like highways.

3.7 Interaction with Onboard Sensors

Sensors are the mode of communications through which data can be fetched for the further communication. Sensors can fetch and process the data related to velocity of the vehicle, direction and can communicate to the nearby data center. Sensors form a good link for communication in routing protocols.

4. VANET Communication Model

As mobile communication has drastically changed the lifestyles of human being, vehicular communication is expected to play a very important role as a future development of the society. Industrial sectors, telecommunication sectors, government research agencies, academic researchers are focusing in developing more secure transportation on the roads through Vehicular Adhoc Networks. VANET is a special case of MANET, in which vehicles equipped with wireless and processing capabilities can create spontaneous network moving along the roads while travelling[20]. Vehicles at the current are also being equipped with on-board computing and wireless communication devices along with specific sensors and navigation systems like Global Positioning System (GPS). Communication in VANET can take place in three different ways as shown in Figure 2 i.e. it can be either V2V or V2I or also both V2V and V2I (hybrid network)[21]. V2V communication uses radio and infrared waves to establish communication. Radio waves have very high frequency (VHF). These can be micro or millimeter waves. When it comes to line of sight communication, infrared and millimeter waves are utilized. Whereas for broadcast communicationVHF and microwaves are preferred.

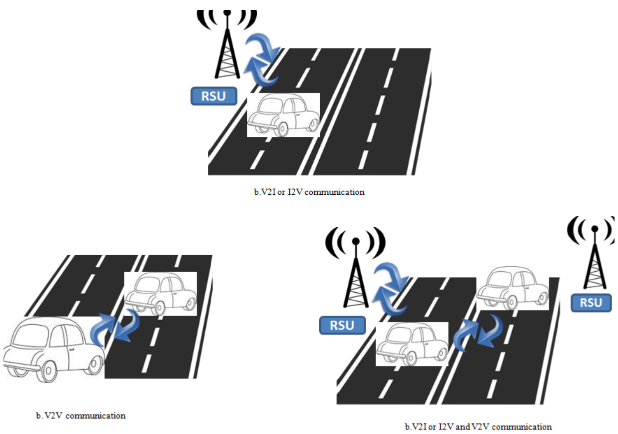

Figure 2. Different types of VANET communication model.

IEEE 802.11 has been reconstructed to IEEE 802.11p for wireless communication in VANET[20]. The basic characteristic of this is as of Wi-Fi, added on with some advanced specification for intelligent transport system. ITS provides aband of 5.9 GHz(5.85-5.925 GHz) for the same[22]. Higher standard based similar to IEEE 802.11p is IEEE 1609 for advanced level applications in VANET. There are various ways of communication through the VANET which includes vehicle to vehicle communication as shown in Figure 2. Here the data or and any other valid information related to security or any message transfer is communicated only between two vehicles. Another way is to communicate between RSU and the vehicle, where data shared is related nearby providing information related to available scenario as shown in Figure 2. Apart from this,in VANET the communication can also take place between all the three different units i.e. RSU to vehicle or also vehicle to vehicle as shown in Figure 2.IEEE 1609 standard defined for communication for Wireless Access in Vehicle Environment (WAVE)has different parts as shown in Figure 3. WAVE 1609.1 section is responsible to establish connection with the on board unit along with a processor section. WAVE 1609.2 defines various secured message structure. These structures are designed in order to protect the message from various attacks. WAVE 1609.3 handles the network services. WAVE 1609.4 it handles multi-channel co-ordination[20]. Not only WAVE, but there are various wireless communication technologies that support vehicular communication. While having communication between the vehicles in an open environment, the security of VANETs is one of the most critical issues as their information transmission is propagated in open access environments. The system should be capable of establishing the liability of drivers but at the same time, it should provide protection as far as possible the privacy of the drivers and passengers are considered[23].Vehicular AdhocNetworks are also easily prone to several vulnerabilities and attacks due to open access communication. These attacks may include Jamming, Forgery, Impersonation, Privacy Authenticationand many more[24,25].

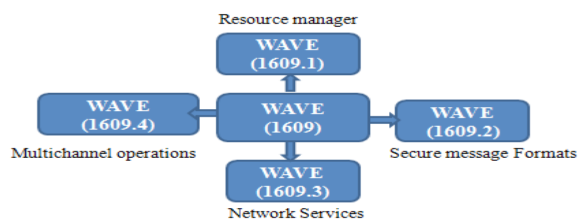

Figure 3. Generalized structure of IEEE 1609 standard.

There are various advantages of various wireless communications technologies for vehicular communication as reflected in Table 1. Various wireless technologies like Wi-Fi, WiMax, WAVE, Infrared, and Cellular can be used for vehicular communication. However, from the table it can be concluded that WiMax offers better radio coverage as well as very high data rate as compared to other technologies but with a compromise of high transmission power for single mobile node. Therefore, for low traffic loads, even at high speed of vehicles we can get low latencies using 802.11p. Different experimental results from[26], WiMax attains better results than 802.11p and 802.11a.

5. Routing Strategies for VANET

Communication between the nodes in an available network is formed during various routing strategies.

Table 1. Comparison of different high speed wireless communication technologies

Indicative wireless features	Wi-Fi	802.11p (WAVE)	Infrared	Cellular	Wimax
Standards	IEEE 802.11	IEEE,ISO,ETSI	ISO	ETSI,3GPP	IEEE 802.16
Channel bandwidth	1–40MHz	10MHz, 20MHz	N/A (optical carrier)	25MHz (GSM), 60MHz (UMTS)	1.25MHz-20MHz
Allocated spectrum	50MHz @ 2.5GHz, 300MHz @ 5GHz	30MHz (EU), 75MHz (US)	N/A (optical carrier)	(Operator-dependent)	2.3GHz,2.5 Ghz,3.5GHz
Frequency band(s)	2.4GHz, 5.2 GHz	5.86–5.92 GHz	835–1 035 nm	800 MHz, 900 MHz, 1800MHz, 1900MHz	2GHz-11GHz
Communication range	< 100 m	< 1 000 m	< 100 m (CALM IR)	< 15km	<50km
Half/full Duplex	Half	Full	Half	Half	Full
Suitability for mobility	Low	High	Medium	High	High
Bit rate	6–54Mb/s	3–27Mb/s	< 1Mb/s <2 Mb/s	< 2Mb/s	100Mbps for 20MHz channel
Transmission power for mobile node	100mW	2 W EIRP (EU), 760mW (US)	12 800 W/Sr pulse peak	380mW (UMTS),2 000mW (GSM)	0.5W-10W

These routing schemes make use of available network and resources to communicate and confirm a faithful transaction among two nodes. Depending upon the scenario used for routing, they are divided into following ways[4].These all routing strategies can be briefly depicted from Table 2.

5.1 Broadcast Routing

Broadcast routing is method wherein the packets are not routed and forwarded by the routers in any network. It is configured to forward the messages in some different ways. A broadcast message is destined to be circulated to all network devices in a particular network. Here the router can send the message to the host one after the other and then the host circulates it among other entities in the network.Another way is that the router just floods the message to all possible networks connected.Some of the protocols used under broadcast routing of vehicular communication include BROADCOMM, Urban Multi-hop Broadcast Protocol (UMB)[27], Vector-Based Tracing Detection(V-TRADE), Distributed Vehicular Broadcast (DV-CAST).As compared to other protocols, V-TRADE and UMB are location based protocols and V-TRADE has more delay constraints than UMB.

5.2 Geocast Routing

Here the transmission of message depends upon the location of a particular vehicle. Normally the group message is send to number of vehicles under same application. It depends upon the application whether the message is to send in group or to a particular node. For transmission of message each node or the vehicle must be capable of identifying its location and convey it to the nearby communication device may be RSU. Some of the Geocast routing protocols for vehicular communication include Inter-Vehicle GeoCast (IVG), Direction-based Geo Cast Routing (DG-CASTOR),Distributed Robust Geo Cast(DRG), Robust Vehicular Routing (ROVER), Dynamic Time-Stable Geo Cast (DTSG), Border node Based Routing (BBR),Vehicular Ad-hoc Networks Context-Aware Routing Protocol (VCARP). The location tracking can be fulfilled through the GPS on board. However, from the above protocols only VCARP and BBR guarantee delivery.

5.3 Cluster Routing

Here the network is divided into sub networks or substructures called as clusters which are interconnected in a network. Each network has a cluster head which

Table 2. Different routing protocols for VANET

Broadcast	Geocast	Cluster	Position		Topology	
BROADCOMM	IVG	CBR	NON-DELAY TOLERANT	GPSR	PROACTIVE	DSDV
UMB	DG-CASTOR	CBLR		GPCR		OLSR
V-TRADE	DRG	HCB		CAR		FSR
DV-CAST	ROVER	COIN		GSR		
	DTSG	LORA-CBF		A-STAR		
	VCARP	CBDRP		GYTAR	REACTIVE	DSR
	BBR	TIBCRPH		CBF		AODV
		MIBR		TO-GO		TORA
			DELAY TOLERANT	GeOpps		
				VASS		
			HYBRID	GeODTN		

helps to circulate the message to the other elements in the network through gateways.Some of the Clustering based protocols for vehicular communication includeCluster Based Routing (CBR), Cluster Based Location Routing (CBLR), HCB, and Clustering for Open IVC.

Network (COIN), Location Routing Algorithm with Cluster Based Flooding (LORA-CBF),Cluster Based Directional Routing Protocol (CBDRP),andTraffic Infrastructure Based Cluster Routing Protocol with Handoff (TIBCRPH), Mobile Infrastructure Based VANET Routing Protocol (MIBR). Cluster based routing protocols are designed for local services and are used by extending the different services by various means like inter-cluster and intra-cluster communication. However, these types of protocols face main challenge in maintenance of varying clusters and dynamic selection of respective cluster heads.

5.4 Position Routing

Position of each node is used for decision of transferring messages to any other node in the network. Depending upon the position the message is been circulated.It is required that a particular node is aware of its own positions in absolute or relative terms as well as its velocity and the direction in which it's moving. Position based routing is further classified as delay tolerant, non-delay tolerant and hybrid routing. These are based on delay specific constraints for delivering the message to a particular node. Some of the position based protocols include Greedy Perimeter Stateless (GPSR), Greedy Perimeter Coordinator Routing (GPCR), CAR, Geographic Source Routing (GSR), Anchor-Based Street and Traffic Aware (A-STAR), Greedy Traffic Aware Routing (GYTAR), Contention Based Forwarding (CBF),Topology -assisted Geo-Opportunistic (TO-GO),Geographical Opportunistic Routing (GeOpps),VASS,Geographic Routing in Disruption Tolerant Networks (GeODTN). Dynamic base station DGPS (DDGPS), is also one of the technique which is used by vehicles in the second step to generate and broadcast the GPS pseudo range corrections that can be used by newly arrived vehicles to improve their positioning[28]. Position based routing methods have a disadvantage of finding out the proper location of the vehicles; this is mainly due to the inaccuracy of some of the GPS location systems.The packet delivery ratio of Geo-Reactive increases when compared with GPSR as packets are forwarded only through stable links[29].

5.5 Topology Routing

As compared to position based routing, topology based routing has limited performance. This scheme effectively requires additional node to carry the topology information during the routing decisions. This routing is further divided in proactive and reactive routing. Some of the topology based routing protocols include Destination-Sequenced Distance-Vector (DSDV), Optimized Link State Routing (OLSR)[30,31], Fisheye State Routing (FSR),Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA). Generally, these protocols are not used well in the terms of VANETs due to the overheads because of routes finding and also due to maintenance ofroutes in the while the vehicle is moving. In VANET scenario the mobility factor is high as the vehicle is in continuous moving condition. This makes a frequent network partitioning which leads to disconnection of routes. As the routes get disconnected the topology information is required to be re-circulated again.To discover routes with the limited routinginformation, a receiver contention scheme is designed fordetermining the next hop[32].

6. Secure Routing Protocols for VANET

There has been various routing protocols communication in VANET as well as to preserve its security aspects. From last few years many researchers have developed and suggested many such approaches that can benefit in time, delay, latency, security, power consumption and many more parameters for secured VANET communication. TCP/IP layer implementation and the threats on different layers of this model have been discussed and solution for the same has been provided in. Also from privacy point of view, a logical address, distinguishes the node within a global area, is the privacy threatening factor. IPv4 and IPv6 packet format and privacy threatening fields are also important to study when establishing VANET communication[33].Denial of Service attack, Message Suppression Attack, Fabrication Attack, Alteration Attack, Replay Attack, Sybil Attack[34], are the attacks which can occur during VANET communication. This may affect the security of the VANET.The survey on various attacks and its possible solutions have been discussed and in [35–37]. Mainly two major attacks on VANETs, Sybil and Denial of service is the most dangerous for VANET. Hence in this scenario, secure data aggregation is must in order to enable a node valid information instead of false. Comparison of various proposed schemes for faulty and misbehaving nodes is made in[38]. Another algorithm of DMN- detection of malicious node in VANETs which improves network performance has been proposed in [39,40]. It isolates the nodes which has abnormal behavior and selects and verifies the node based on three values i.e. load, distance and discrete trust value.Special case of Sybil attack detection through active position detection has been proposed in[41].The identity based signature scheme proposed in[42] is more effective in time consumption. It uses Elliptical Curve Cryptography (ECC) algorithm for its implementation. Various requirements like, authentication, traceability of trusted third party, integrity of message, driver likability and batch signature verification has been supported by this algorithm. Identity Based Batch Verification (IBV), for secured and efficient use in VANET communication also proposed in [43]. Here it provides good performance in terms of delay and transmission overhead.Identity based cryptographic solution provide authentication, confidentiality, non-repudiation and message integrity[44]. Here no extra storage is required for any of the vehicles neither for the infrastructure. Verification of a new node entering the network must be done to ensure that the node is trusted. To validate this information, each node sends a vector to show its recommended trusted value. Based on this the false node is eliminated from the network. This mechanism is proposed in[45]. Not only recognition of unknown node is essential, but balanced overhead for computation and secured guarantee from attacks is also important. The same has been explored in with RSU in[46]. Apart from this authentication of transferring node with privacy preserving is proposed in[47]. It also describes the better performance of ECC over Rivest Shamir and Adleman (Encryption algorithm-RSA) in context with two important factors which includes key size and computation. As authentication of node entering the network is important, [48]proposes a scheme of multiple base stations, where the base station checks and verifies the identification of each node using the vehicle identification number. Group based authentication is also safe and effective for safety message dissemination[49]. Another access control scheme for vehicular communication with thehelp of we integrate pseudonym with Identity Based Signature (IBS) is proposed in[50]. It authenticates the message and exploits pseudonym to protect privacy.The efficiency of data access was improved by allowing sharing and coordination of cached data using pseudonym based cryptography in[51]. Batch verification is also added on in this algorithm. Biometrics plays an important part in identification and authentication. A combination of face and finger print biometrics provide more accurate recognition of users.[52]Proposes, a novel approach for enhancing the security of user authentication in VANETs based on biometrics. Entry of malicious node is expected during VANET communication. Hence trust building isanother method to authenticate the user[53,54]. [55]gives a systematic review of various trust management schemes implemented for effective VANET communication. Signature based approaches helps to establish better trust in terms of authentication. The Road Side Controller (RSC) controls the RSU and also the delivering of messages through the RSU to any vehicle in a particular area. [56]uses proxy signature mechanism based on ECC for authentication.Evaluation of better performance during RF jamming attacks is difficult to obtain. VANET communication has to compromise road safety during RF jamming. The protocol which can detect and mitigate RF jamming attacks has a broad research future[57]. Elliptic Curve Digital Signature Algorithm (ECDSA) and AES can also be designed for secured routing. These methods have highest packet receiving ratios, even AES is superior then all methods, it increased the probability of message receiving in emergency case[58].

Heterogeneousarea is the most demanding areas for VANET research. A prerecorded co-operative transmission scheme that can effectively extract the underlying Doppler spatial diversity is proposed in[1]. This proposed technique requires less power transmission as compared with the traditional schemes also it has been observed that it give increased distance coverage. This scheme proposes networking at its best for highly populated urban areas. By using a minimum hop count prediction, better performance in terms of end to end delay and packet delivery ration for heterogeneous network is seen in[59]. Selection of appropriate gateway to establish the connection with source vehicle is also an efficient task. A fuzzy logic QoS based scheme for appropriate selection of gateway is proposed in[17]. The results of this also providebetter progress than the other deterministic schemes for selection of gateway. Another fuzzy logic based Fuzzy Logic based Greedy Routing (FLGR) protocol has been proposed which assists in delivering safety messages to the destination vehicle with minimum delay[60]. [61]proposesan optimized model for multi-hop adhoc network to select the position of gateway over a certain area. Multi hop clustering scheme with improves stability is obtained in[62]. The distributed manner selecting of target leads to efficient and easy cluster structure. Cloud computing provides sharing of large data and resources over a media called as cloud. This sharing of data through clouds can also be used by VANET for its communication. Large data storage, services like software, computational infrastructure, at a reduced cost in been proposed in[63].This approach is based on two models of clouds i.e. permanent and temporary. Traffic Information as a Service (TIaaS), is another cloud based service proposed in[64,65]. This algorithm preserves the most important parameters of VANETi.e., authentication,integrity and non-frame ability. Privacy preserving during VANET communication in order to protect from various attacks has been proposed in[66–68]. Here collecting of traffic information and road status for safety is obtained through VANET[69].Secure Traffic Congestion Control Protocol (SCOOL) proposed in[70] is a secure routing protocol which provides integrity and authenticity of transmitted data.Position based routing of VANET is another way of communication for VANET. Various protocols like non-delay tolerant[71], delay tolerant[72], hybrid protocols including Gpsrj+, JARR,GyTAR,GSR,SKVR, VADD and many more has been explained in[73]. An Improving Positioning in real City environments IPC algorithm that can reduce the GPS position errors has been proposed in[74]. This protocol improves location accuracy.Comparative analysis of location based routing using Location Aided Routing (LAR) and Zone Routing Protocol (ZRP) protocols are also reviewed in[75]. Another approach of co-operative map matching method based on dynamic Base Station (DGPS) is also used for improved position. It is decentralized method for improvement in GPS positioning. Other various position based protocols for improved security has been discussed in[76,77]. Depending on the scenario of large traffic and parking based problems, [78,79]tries to propose a solution to this using dissemination scheme for VANETs. Another recent approach includes Neighbor Discovery Algorithm based on local monitoring to improve the security of the data packets being transmitted by vehicles and therefore avoiding collision attack in VANET.

The challenge in providing the effective routing protocol involves, the low communication delay, low communication overhead[80], low time complexity. To meet these aspects there are various protocolsbased on their strategy, based on target on which the protocols works, and many more. All these protocols are reviewed in[81–83],[83]geocast routing is a strategy based protocol. DRG protocol is effective and gives better performance for urban areas. Stable CDS-Based Routing Protocol (SCRP) a stable CDS based routing protocol is also suitable for urban areas tries to sole the addresses issue of selecting routing paths with minimum end-to-end delay[84]. It provides minimum end to end delay for non-safetyapplication. In[85] it has been proposed that with the effect of DRG the vehicle speed has reduced as it comes close to the incident zone. Location Information Verification Cum Security (LIVES) based on Transferable Belief Model (TBM) also uses geocast routing strategy for communication between vehicles. The increment in location error probability is lower in case of LIVES as compared to A-VIP and W-LIVES[86]. Based on network model, geographic location privacy scheme which uses identification location privacy threatening factors, along with its solutions is proposed in[4,87]. However this approach still lacks behind the in providing authentication. Fair access to V2 communication including collision free transmission must be ensured along with security. The Bayesian Trusted Effective Routing (BTER) scheme provides a trust management mechanism between the nodes in the VANET routing process[88].However, the theory of belief functions is more rich and flexible than its Bayesian counterpart, however it is more computationally demanding[89]. A new RSU selection algorithm, named RSEL has been proposed for the same in[90]. Here the RSU load was improved up to 50%. CR-VANETs, [91–94]are also a new technology in Vehicular Adhoc Network. This technology satisfies the demands of video and audio streaming, collision warning, gaming and many more. The results in[93] demonstrated that MOCA can enhance connectivity in vehicular cognitive networks and outperformed the other approach in terms of throughput and jitter.

7. VANET Security Aspects

When it comes to working of Adhoc Networks with co-operative transmission, security and privacy aspects must be taken into consideration to achieve the effective results. While considering these main requirements to fulfill by the system is to provide with following things[15,95]:

- Availability
- Integrity
- Confidentiality
- Privacy
- Authentication
- Non-Repudiation
- Freshness

Security requirements are well described in[96]. Not only this, but the efficiency of these nodes be up to mark due to its mobile node functionality. It is possible that other types of attack may occur when VANETs are actually implemented in the real world[12]. To secure VANETs from attacks, the main discovery must be made up of different types of attackers. These attackers can be broadly classified as follows[14], Insider and Outsider or Malicious and Rational or Active and Passive. Once the process of harming the system by the attacker is known, it becomes easy to understand and detect the attack. Secured possible solutions on some attacks have been proposed in[22,24,97]. But still the system requires many robust techniques to achieve secured and privacy preserved data migration. Some of the techniques provide hardware level security while others may provide just data related security. However, it depends on the application for which the system is designed. Table 3 shows the different security techniques and their advantages and disadvantages. However, many advanced version techniques to provide high level, all round security are under research.

With the consideration of different security aspects and the recent study for the implementation of VANET using different algorithms and strategies, Table 4 has been constructed. This table tries to explore the advantages and disadvantages of the various security papers implemented for fulfilling the security need.

Table 3. Theoretical analysis of different security[95]

Technique	Year of Development	Advantages	Disadvantages	Level of security
Authentication	1984	Use encryption, hash function, digital signature and certificates.	Difficult to authenticate entity	Authentication level
Group signature	1991	Any group member can sign the message	Any attacker node can access the information of the group	Group based
Detection and correction of malicious data	2004	Node to node communication	Passive node attack	Data level
Hardware security	2008	Use cryptography protocols	Programs and contents running on its own is not secure	Hardware level
Public key infrastructure	2010	Private key is kept with encrypted message	Malicious node can access the public key of the sender	Certificate authority
Certificate revocation	2010	Maintains the record of all revoked keys	User no longer possess the private key	Certificate based

8. Simulation Platform

In recent years wireless and mobile network have been in vast usage and has become as a daily necessity of human being. It also increases its importance by providing various facilities in short time span.By providing safety and quick information VANETs have gained attraction towards research. Simulators play a very important role while judging the performance in real time scenario considering various aspects of VANET communication. These simulators can be broadly classified as Network Simulators, Traffic Simulators and VANET Simulators. These simulators must be capable of analyzing the speed limits, number of lanes, traffic signals, lights, overtaking scenario and should consider the safety rules.

8.1 Network Simulators

Whenever there is a communication to be established in a network, network simulation is a good technique

Table 4. Survey of Advantages and disadvantages for various security algorithms

Sr. No	Reference	Advantage	Disadvantage
1	41	Preventing Sybil attacks	Detect all compromised vehicle yet not focused
2	46	Less overhead,less time consumption and authentication	Confidentiality ,Privacy aspects not considered
3	48	Athenticaton is provided through VIN(gaureented authentication)	V2I not focused
4	74	Improve the localization error	Video shortcomings such as image quality
5	42	Efficient time consumption	Confidentiality ,Privacy aspects not considered
6	45	Accurately validate the vehicle node	Historical events needs to be stored
7	47	Amount of Data Transfer and time is reduced	Confidentiality ,Privacy aspects not considered
8	49	5 aspects of security considered	Fake Group leaders or any vehicle left the group is not insvestigated here
9	52	Gives Authentication and biometrics template, also it resists multiple attacks	Confidentiality ,Privacy aspects not considered
10	43	independent of the number of message signatures,decrease the time cost, better scalability	Illegal signatures not verified
11	67	Authentication,integrity,non-repudation for both service provider and vehicle,false request can be identified	Confidentiality ,Privacy aspects not considered
12	86	Error probabilty less and end to end delay decreases	Non-adversary vehicles is not considered
13	54	Ensures anonymity and privacy	Lifetime of private pseudonym and pseudonym change w.r.t distance travelled must be focused
14	70	Communication overhead is less,gaurantees privacy and authentication	Only authorized units can be linked and can transfer the data
15	31	Does not requires pre-registered identities	Large size of network and sybil attack is not considered
16	39	Fake node detection,improvedthroughput,better packet delivery ratio,reduced end to end delay	Prevention from malicious node not focused
17	64	less time-consuming,authentication,privacy and confidentiality	Processing and communication delay to the clouds must be defined
18	68	Provides authentication,anonymity and anonymous vehicle tracing	Confidentiality aspect not considered
19	50	Supports confidentiality,access control and authentication	Decryption efficiency not specified
20	40	Better detection ratio,new path identification	Different aspects of security can also be added(not considered here)
21	34	Message integrity and privacy preserved	Automatic establishement of trust is not focused

wherein a program examines the behavior of a network. This can be done either by communicating through various entities of within the network or by even various mathematical calculations and observation. There is large amount of network simulators designed for various VANET applications. These simulators work on various programming language including C++, JAVA. Depending upon the application and the required security these simulators are available either as open source or for commercial need. Some of these simulators include NS2,GloMoSim,OMNet ++,JiST/SWANS under the open source category. OPNet and QualNet[84,98–100] are commercial network simulators.

8.2 Traffic Simulators

As in deal with VANET, traffic plays a very important part. This traffic may vary depending upon the speed of the vehicles. However there and simulation platforms which provide the analysis based on the available or the current traffic of the network. This analysis may include a better plan for a good traffic flow. Also it may be used for future traffic prediction results and their uses. Even these simulators, depending upon the programming requirement are either open source or commercial based. Some of these may include VanetMobisim, Sumo, MOVE, STRAW, CityMob under the open source category. Paramics is one of the traffic simulators for commercial applications.

8.3 VANET Simulators

These simulators are a combination of both network and traffic simulators. Therefore, these simulators give the analysis of the created network environment and also the current traffic analysis.TraNS is the VANET simulator having a combination of NS2 and SUMO. OtherVANET simulators are GrooveNet and NCTUS. These are open source VANET simulators.

9. Future Research Direction

As per table 5, the security aspect like availability, integrity and non-repudiation has not yet been focused. These aspects if not considered may cause an attack to harm the security of the system.Up to date, there are no security standards that sufficiently meet all security requirements with fewer overheads[101]. Future research direction should

Table 5. Future research direction to focus on possible security aspects to be fulfilled

<table>
<tr><th>Sr. no</th><th>Reference</th><th>Year</th><th>Confidentiality</th><th>Integrity</th><th>Authentication</th><th>Availability</th><th>Non-repudiation</th><th>Privacy</th></tr>
<tr><td>1</td><td>41</td><td>2008</td><td rowspan="6">Not Defined</td><td>Not Defined</td><td rowspan="15">Yes</td><td rowspan="6">Not Defined</td><td>Not Defined</td><td rowspan="5">Not Defined</td></tr>
<tr><td>2</td><td>46</td><td>2011</td><td>Yes</td><td>Yes</td></tr>
<tr><td>3</td><td>48</td><td>2012</td><td>Not Defined</td><td rowspan="4">Not Defined</td></tr>
<tr><td>4</td><td>42</td><td>2015</td><td>Yes</td></tr>
<tr><td>5</td><td>45</td><td>2015</td><td rowspan="2">Not Defined</td></tr>
<tr><td>6</td><td>47</td><td>2015</td><td>Yes</td></tr>
<tr><td>7</td><td>49</td><td>2015</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td rowspan="4">Not Defined</td></tr>
<tr><td>8</td><td>52</td><td>2015</td><td rowspan="7">Not Defined</td><td rowspan="2">Not Defined</td><td rowspan="12">Not Defined</td><td rowspan="2">Not Defined</td></tr>
<tr><td>9</td><td>43</td><td>2015</td></tr>
<tr><td>10</td><td>67</td><td>2015</td><td>Yes</td><td>Yes</td></tr>
<tr><td>11</td><td>54</td><td>2015</td><td rowspan="4">Not Defined</td><td rowspan="6">Not Defined</td><td rowspan="2">Yes</td></tr>
<tr><td>12</td><td>70</td><td>2015</td></tr>
<tr><td>13</td><td>31</td><td>2015</td><td rowspan="2">Not Defined</td></tr>
<tr><td>14</td><td>39</td><td>2015</td></tr>
<tr><td>15</td><td>64</td><td>2015</td><td>Yes</td><td>Yes</td><td rowspan="2">Yes</td></tr>
<tr><td>16</td><td>68</td><td>2015</td><td>Not Defined</td><td>Not Defined</td><td>Yes</td></tr>
<tr><td>17</td><td>51</td><td>2015</td><td rowspan="2">Yes</td><td>Yes</td><td>Not Defined</td><td>Yes</td><td rowspan="2">Not Defined</td></tr>
<tr><td>18</td><td>50</td><td>2016</td><td>Not Defined</td><td rowspan="2">Yes</td><td rowspan="2">Not Defined</td></tr>
<tr><td>19</td><td>34</td><td>2016</td><td>Not Defined</td><td>Yes</td><td>Yes</td></tr>
</table>

focus consideringtheavailability, integrity and non-repudiation along with authentication for security in VANET. Although much development has taken place, security aspectsstill lag behind. Real time applications of these techniques can be employed to find out the correct performance to that of the simulated results[102].Table 5 indicates the various future research direction which should be considered so that a secured VANET without any possible attack can be proposed.

10. References

1. Feteiha M, Hassanein H. Enabling cooperative relaying VANET clouds over LTE-A networks.IEEE Transactions on Vehicular Technology; 2015. p. 1468–79.
2. Boyaci A, Zaim H, Sonmez C. A cross-layer adaptive channel selection mechanism for IEEE 802.11P suite. Journal on Wireless Communications and Networking; 2015.
3. Mir ZH, Filali F. LTE and IEEE 802.11p for vehicular networking: A performance evaluation.EURASIP Journal on Wireless Communications and Networking; 2014. p. 89.
4. BhoiS,Khilar P.Vehicular communication: A survey. IET Networks. 2014; 3(3):204–17
5. Xiong W, Xu J, Li Y, Zhao N, Wan X, Liang J.Minimum node degree of k-connected vehicular ad hoc networks in highway scenarios. Journal on Wireless Communications and Networking; 2016.
6. Ahmed S, Ariffin S, Fisal N. Network coding techniques for VANET advertising applications.Journal on Wireless Communications and Networking. 2015; 1.
7. ZeadallyS, HuntR,Chen Y,Irwin A, Hassan A. Vehicular Ad hoc Networks (VANETS): Status, results, and challenges. Telecommunication Systems. 2010; 50(4):217–241.
8. Dressler F, Altintas O, Scheuermann B, Banerjee S. Special issue on advances in vehicular networks.Ad Hoc Networks. 2016; 37:1–2.
9. Eze E, Zhang S,Liu E,EzeJ. Advances in Vehicular Ad-hoc Networks (VANETs): Challenges and road-map for future development.International Journal of Automation and Computing; 2016. p. 1–18.
10. Daniel A, Paul A, Ahmad A, Rho S.Cooperative intelligence of vehicles for Intelligent Transportation Systems (ITS). Wireless Personal Communications; 2015. p. 461–84.
11. Masini B, MolinaroA,Costa L, Sukuvaara T, DucourthialB. Vehicular networking for mobile crowd sensing.Ad Hoc Networks; 2016. p. 407–8.
12. Engoulou R, BellaÃiche M, Pierre S, Quintero A. VANET security surveys.Elsevier. 2014:1–13.
13. Mejri M, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions.Vehicular Communications. 2014:53–66.
14. Singh A, Kad S. A review on the various security techniques for VANETs.Procedia Computer Science; 2016. p. 284–90.
15. Di Pietro R, Guarino S, Verde N, Domingo-Ferrer J. Security in wireless ad-hoc networks:A survey.Computer Communications; 2014. p. 1–20.
16. Al-Sultan S, Al-Doori AM,Al-Bayatti H,Zedan Z. A comprehensive survey on vehicular AdHoc network.Elsevier. 2013; 37:380–92.
17. Zhioua G, Tabbane N, Labiod,Tabbane S. A fuzzy multi-metric QoS-balancing gateway selection algorithm in a clustered VANET to LTE advanced hybrid cellular network.IEEE Transactions on Vehicular Technology; 2015. p. 804–17.
18. Campolo C,Molinaro A, Scopigno R. From today's VANETs to tomorrow's planning and the bets for the day after. Vehicular Communications. 2015; 2(3):158–71.
19. Kumar V, Mishra S, Chand N. Applications of VANETs: Present and Future, Communications and Network. 2013; 5(1B):12–15.
20. Cunha F, Villas L, BoukercheA,Maia G, Viana A, Mini R, Loureiro A. Data communication in VANETs: Protocols, applications and challenges, Ad Hoc Networks; 2016. p. 90–103.
21. Saravanan D, Agalya V, Amudhavel J, Janakiraman S. a brief survey on performance analysis and routing strategies on Vanets. Indian Journal of Science and Technology. 2016 Mar; 9(11):1–6.
22. Raw RS, Singh KM. Security challenges, issues and their solutions forVanet.International Journal of Network Security andits Applications. 2013:95–105.
23. Nasir MK, Hossain A, Hassan M, Ali M. Security challenges and implementation mechanism for vehicular ad hoc network.International Journal of Scientific & Technology Research. 2013:156–61.
24. ErtaulL,Mullapudi S. The security problems of Vehicular Ad hoc Networks(VANETs) and proposed solutions in securing their operation.DBLP Conference: Proceedings of the 2009 International Conference on Wireless Networks, ICWN 2009, Las Vegas Nevada, USA; 2009. p. 13–16.
25. Mohanty S, Jena D. Secure data aggregation in Vehicular-Adhoc Networks: A survey.Procedia Technology; 2012. p. 922–9.
26. Fernández-Caramés T, González-López M, Castedo L.Mobile WiMAX for vehicular applications: Performance evaluation and comparison against IEEE 802.11p/a. Computer Networks; 2011. p. 3784–95.
27. Rahim A, Muhaya FB, Sher M, Khan ZS, Ahmad I. Performance evaluation of broadcast techniques in VANETs. Indian Journal of Science and Technology. 2009 Oct; 2(10):1–4.
28. Rohani M, Gingras D, Gruyer D. A novel approach for improved vehicular positioning using cooperative map matching and dynamic base station DGPS concept. IEEE Transactions on Intelligent Transportation Systems;2016. p. 230–9.
29. Darisini PSN, Kumari NS. Geo-reactive: An efficient and reliable hybrid routing protocol forVANETs. Indian Journal of Science and Technology. 2015 Oct; 8(27):1–6.

30. Kanchanasut K, Boonsiripant S, Tunpan A, Kim H, Ekpanyapong M. Internet of cars through commodity V2V and V2X mobile routers: Applications for developing countries. KSCE Journal of Civil Engineering; 2014. p. 1897–1904.
31. Gantsou D. Invited Paper: VANET security: Going beyond cryptographic-centric solutions. Chapter Vehicular ad-hoc networks for smart cities,of the series Advances in Intelligent Systems and Computing; 2015. p. 43–9.
32. MokhtarB,Azab M. Survey on security issues in vehicular ad hoc networks. Alexandria Engineering Journal; 2015. p. 1115–26.
33. Lim HJ, Chung TM. A survey on privacy problems and solutions for VANET based on network model.Springer-Verlag Berlin Heidelberg; 2011. p. 74–88.
34. Feng X, Li C, Chen D,Tang J. A method for defensing against multi-source Sybil attacks in VANET.Peer-to-Peer Networking and Applications; 2016.
35. Samara G, Al-Salihy WAH, Sures R. Security analysis of Vehicular Ad Hoc Networks (VANET).ACM,NETAPPS '10 Proceedings of the 2010 Second International Conference on Network Applications, Protocols and Services; 2010. p. 55–60.
36. Balasubramani S, Rani S, Rajeswari KS. Review on security attacks and mechanism in VANET and MANET.Springer India,Artificial Intelligence and Evolutionary Computations in Engineering Systems, Advances in Intelligent Systems and Computing;2016. p. 655–66.
37. Sumra IA, Bin Hasbullah H, Bin AbManan J. Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey.Vehicular Ad-hoc Networks for Springer. Smart Cities, Advances in Intelligent Systems and Computing; 2015. p. 51–61.
38. Rivas DA, BarcelÃ³-Ordinas J, Zapata MG, Morillo-Pozo J. Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation.Journal of Network and Computer Applications; 2011. p. 1942–55.
39. 39.Khan U, Agrawal S, Silakari S. Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks.Procedia Computer Science; 2015. p. 965–72.
40. Rupareliya J, Vithlani S, Gohel C. Securing VANET by preventing attacker node using watchdog and bayesian network theory.Procedia Computer Science; 2016. p. 649–56.
41. 41.Yan G, Olariu S, Weigle M. Providing VANET security through active position detection.Computer Communications; 2008. p. 2883–97.
42. Lo N, Tsai J. An efficient conditional privacy-preserving authentication scheme for Vehicular Sensor Networks without pairings.IEEE Transactions on Intelligent Transportation Systems; 2015. p. 1–10.
43. Horng S, Tzeng S, Li T, Wang X, Huang P, Khan M. Enhancing security and privacy for identity-based batch verification scheme in VANET.IEEE Transactions on Intelligent Transportation Systems; 2015. p. 1–1.
44. Kamat P, Baliga A, Trappe W. An identity based security framework for VANETs.ACM; 2016. p. 94–5.
45. Zhou A, Li J, Sun Q, Fan C, Lei T, Yang F. A security authentication method based on trust evaluation in VANETs. EURASIP Journal on Wireless Communications and Networking; 2015, p. 59.
46. Wu H, Hsieh W. RSU-based message authentication for vehicular ad-hoc networks.Multimedia Tools and Applications; 2011. p. 215–27.
47. Singh K, Saini P, Rani S, Singh AK. Authentication and privacy preserving message transfer scheme for Vehicular Ad Hoc Networks (VANETs).Proceedings of the 12th ACM International Conference on Computing Frontiers;2015.
48. Mondal A, Mitra S. Identification, authentication and tracking algorithm for vehicles using VIN in centralized VANET.Advances in Communication, Network, and Computing; 2012. p. 115–20.
49. Hasrouny H, Bassil C, Samhat A, Laouiti A. Group-based authentication in V2V communications.2015 Fifth International Conferenceon Digital Information and Communication Technology and its Applications (DICTAP); 2015. p. 173–7.
50. Kang Q, Liu X, Yao Y, Wang Z, Li Y. Efficient authentication and access control of message dissemination over vehicular ad hoc network.Neurocomputing; 2016. p. 132–8.
51. Wang C, Shi D, Xu X, Fang J. An anonymous data access scheme for VANET using pseudonym-based cryptography. Journal of Ambient Intelligence and Humanized Computing. 2015:63–71.
52. Remyakrishnan P, Tripti C. A novel approach for enhancing the security of user authentication in VANET using biometrics.Advances in Intelligent Systems and Computing. 2015; 338:299–306.
53. Patel N, Jhaveri R. Trust based approaches for secure routing in VANET: A survey. Procedia Computer Science; 2015. p. 592–601
54. Moghraoui K, Amar Bensaber B. An efficient pseudonym change protocol based on trusted neighbours for privacy and anonymity in VANETs.DIVANet '15 Proceedings of the 5th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications,ACM; 2015. p. 93–9.
55. Mandala S. Trust management in vehicular ad hoc network: a systematic review.EURASIP Journal on Wireless Communications and Networking. 2015.
56. Biswas S, Misie J. Establishing Trust on VANET Safety Messages. ADHOCNETS; 2010. p. 314–27.
57. Punal O, Pereira C, Aguiar A, Gross J. Experimental characterization and modeling of RF jamming attacks on VANETs.IEEE Transactions on Vehicular Technology; 2015. p. 524–40.
58. Wagan A, Mughal B, Hasbullah H. VANET security framework for safety applications using trusted hardware.Communications in Computer and Information Science; 2011. p. 426–39.
59. Wang C, Chiou Y,Liaw G. Nexthop selection mechanism for nodes with heterogeneous transmission range in VANETs. Computer Communications; 2015. p. 22–31.
60. Agrawal S, Raw RS, Tyagi N, Misra AK. Fuzzy Logic based

Greedy Routing (FLGR) in multi-hop vehicular ad hoc networks. Indian Journal of Science and Technology. 2015 Nov; 8(30):1–14.
61. Urquiza-Aguiar L, Vázquez-Rodas A, Tripp-Barba C, Mezher AM, Igartua MA, Llopis LD. Efficient deployment of gateways in multi-hop ad-hoc wireless networks.PE-WASUN '14 Proceedings of the 11th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, andUbiquitous Networks; 2014. p. 93–100.
62. Chen Y, Fang M, Shi S, Guo X,Zheng X. Distributed multi-hop clustering algorithm for VANETs based on neighborhood follow. EURASIP Journal on Wireless Communications and Networking. 2015.
63. Bitam S, Mellouk A, Zeadally S. VANET-cloud: A generic cloud computing model for vehicular Ad Hoc networks. IEEE Wireless Communications; 2015. p. 96–102.
64. Hussain R, Rezaeifar Z, Lee Y, Oh H. Secure and privacy-aware traffic information as a service in VANET-based clouds.Pervasive and Mobile Computing; 2015. p. 194–209.
65. Jelassi S, Bouzid A, Youssef H. QoE-driven video streaming system over cloud-based VANET.Springer International Publishing Switzerland; 2015. p. 84–93.
66. Malina L, Hajný J, Zeman V. Group signatures for secure and privacy preserving vehicular ad hoc networks. Q2SWinet '12 Proceedings of the 8th ACM Symposium on QoS and Security for Wireless and Mobile Networks,ACM; 2012. p.71–4.
67. Zhang L, Wu Q, Qin B, Domingo-Ferrer J, Liu B. Practical secure and privacy-preserving scheme for value-added applications in VANETs.Computer Communications; 2015. p. 50–60.
68. Yang C, Qin B, Zhou X, Sun Y, He S, Wu Q. Privacy-preserving traffic monitoring in vehicular ad hoc networks. IEEE, International Conference on Advance Networking and Applications Workshops; 2015. p. 22–4.
69. Wongdeethai S, Siripongwutikorn P.Collecting road traffic information using vehicular ad hoc networks. EURASIP Journal on Wireless Communications and Networking. 2016; 1.
70. Younes M, Boukerche A. SCOOL: A secure traffic congestion control protocol for VANETs.IEEE Wireless Communications and Networking Conference (WCNC); 2015. p. 1960–5.
71. Balasubramani, Karthikeyan L, Deepalakshmi V. Comparative study on non-delay tolerant routing protocols in vehicular networks.Procedia Computer Science; 2015. p. 252–7.
72. Sobin CC, Raychoudhury V, Marfia G, Singla A. A survey of routing and data dissemination in Delay Tolerant Networks. Journal of Network and Computer Applications. 2016.
73. Sharef B, Alsaqour R, Ismail M.Comparative study of variant position-based VANET routing protocols. Procedia Technology; 2013. p. 532–9.
74. Tsai M, Wang P, Shieh C, Hwang W, Chilamkurti N, Rho S, Lee Y. Improving positioning accuracy for VANET in real city environments.The Journal of Supercomputing; 2014. p. 1975–95.
75. Husain A, Sharma S. Comparative analysis of location and zone based routing in VANET with IEEE802.11p in City Scenario, Computer Engineering and Applications (ICACEA), 2015 IEEE International Conference on Advances; 2015. p. 294–9.
76. Liu J, Wan J, Wang Q, Deng P, Zhou K, Qiao Y. A survey on position-based routing for vehicular ad hoc networks. Telecommunication Systems; 2015. p. 15–30.
77. Kumar S, Verma A. Position based routing protocols in VANET: A survey.Wireless Personal Communications; 2015. p. 2747–72.
78. Singh G, Chakrabarty N, Gupta K. Traffic congestion detection and management using Vehicular Ad-hoc Networks (VANETs) in India.International Journal of Advanced Computer Technology. 2014:19–26.
79. Salvo P, Cuomo F, Baiocchi A, Rubin I. Investigating VANET dissemination protocols performance under high throughput conditions.Vehicular Communications; 2015. p. 185–94.
80. Huo Y, Liu Y, Ma L, Cheng X, Jing T. An enhanced low overhead and stable clustering scheme for crossroads in VANETs.EURASIP Journal on Wireless Communications and Networking. 2016.
81. Cheng J, Cheng J, Zhou M, Liu F, Gao S, Liu C.Routing in internet of vehicles: A review. IEEE Transactions on Intelligent Transportation Systems. 2015; 16(5):2339–52.
82. Jayachandran S, DoraisamiJothi J, Krishnan S. A case study on various routing strategies of VANETs. Communications in Computer and Information Science; 2012. p. 353–62.
83. Lin Y, Chen, Lee S. Routing protocols in vehicular ad hoc networks: A survey and Future perspectives. Journal of Information Science and Engineering; 2010. p. 913–19.
84. Cheng C, Tsao S. Adaptive lookup protocol for two-tier VANET/P2P information retrieval services.IEEE Transactions on Vehicular Technology; 2015. p. 1051–64.
85. Orozco AM, Céspedes S, Michoud R, Llano G. Design and simulation of a collision notification application with geocast routing for car-to-car communications.European Transport Research Review. 2015:4.
86. Sheet D, Kaiwartya O, Abdullah A, Hassan A. Location information verification cum security using TBM in geocastrouting. Procedia Computer Science; 2015. p. 219–25.
87. Khandelwal S, Jawandhiya P. Safe geo graphic location privacy scheme in the VANETs-survey methods and its limitation.International Journal of Scientific and Engineering Research; 2013. p. 1507–11.
88. Kim S. Timed bargaining-based opportunistic routing model for dynamic vehicular ad hoc network. EURASIP Journal on Wireless Communications and Networking. 2016: 1.
89. Farah MB, Mercier D, Delmotte F, LefèvreÉ. Methods using belief functions to manage imperfect information concerning events on the road in VANETs.Transportation Research

Part C: Emerging Technologies. Journal of Network and Computer Applications. 2011:1942–55.
90. Hoeft M, Rak J. How to provide fair service for V2I communications in VANETs? Ad Hoc Networks; 2016. p. 283–94.
91. Abbassi S, Qureshi I, Abbasi H, Alyaie B. History-based spectrum sensing in CR-VANETs.EURASIP Journal on Wireless Communications and Networking. 2015.
92. Tabassum M, Razzaque M, Hassan M, Almogren A, Alamri A. Interference-aware high-throughput channel allocation mechanism for CR-VANETs.EURASIP Journal on Wireless Communications and Networking. 2016.
93. Silva C, Nogueira M, Kim D, Cerqueira E, Santos A. Cognitive radio based connectivity management for resilient end-to-end communications in VANETs. Computer Communications; 2016. p. 1–8.
94. Qureshi M, Noor R, Shamshirband S, Parveen S, Shiraz M, Gani A.A survey on obstacle modeling patterns in radio propagation models for vehicular ad hoc networks.Arabian Journal for Science and Engineering. 2015. p. 1385–407.
95. Kaur N, Kad S. A review on security related aspects in vehicular ad hoc network.Procedia Computer Science;2016. p. 387–94.
96. de Fuentes JM, González-Tablas AI, Ribagorda A. Overview of security issues in Vehicular Ad-hoc Networks.2010.
97. Dak A, Yahya S, Kassim M.A survey on security challenges in VANETs.International Journal of Computer Theory and Engineering; 2012. p. 1007–10.
98. Kaur M, Singh P. Performance evaluation of V2Vcommunication by implementing security algorithm in VANET. Advances in Computing and Information Technology; 2012. p. 757–63.
99. Chandramohan K, Kamalakkannan P. An efficient neighbor discovery and aloha based collision detection and correction in VANET. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–9.
100. Bala R, Krishna C. Scenario base performance analysis of AODV and GPSR routin protocols in a VANET.2015 IEEE International Conferenceon Computational Intelligence and Communication Technology (CICT); 2015. p. 432–7.
101. ElsadigMA, Fadlalla YA. VANETs security issues and challenges: A survey. Indian Journal of Science and Technology. 2016.
102. Jaiganesh S, Jarina S, Amudhavel J, Premkumar K, Sampathkumar S, Vengattaraman T. Performance analysis of collision avoidanceframe works in VANETS. Indian Journal of Science and Technology. 2016.